

TITLE OF THE INVENTION

**Cryptocommunication system, transmission apparatus, and reception apparatus**

5 This application is based on an application No. 2000-384835 filed in Japan, the content of which is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

10 (1) Field of the Invention

The present invention relates to an encryption technology used as an information security technology, and especially to a technology for detecting errors that occur in decrypting.

15 (2) Related Art

As data communication using a computer technology or a communication technology becomes widespread, cryptocommunication systems are becoming prevalent. The cryptocommunication enables data communication without revealing the communications to a third party who is not an intended party.

Cryptosystems are used for realizing the cryptocommunication systems. In cryptosystems, for generating ciphertext, an authentic encryption key is used in applying an encryption algorithm to plaintext, and for generating decrypted

text, an authentic decryption key is used in applying a decryption algorithm to the ciphertext. In some cryptosystems, there is a possibility of generating decrypted text which is different from original plaintext. Hereafter, the phenomena in which generated decrypted text is different from its original plaintext is referred to as "decryption error," and the cryptosystem in which this decryption error occurs is referred to as "decryption error vulnerable cryptosystem."

One example of the above mentioned decryption error vulnerable cryptosystems is a NTRU cryptosystem. The NTRU cryptosystem, to put it simply, generates ciphertext by encrypting plaintext using random numbers as parameters and using an encryption key, and generates decrypted text by decrypting the ciphertext using a decryption key. This system, using random numbers as parameters, has a chance of obtaining different ciphertext from the same plaintext.

For a detailed description of the NTRU cryptosystem, please refer to Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem," Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998.

In the cryptocommunication system using the NTRU cryptosystem, there is a possibility of obtaining different decrypted text from the original plaintext, therefore intended information is not insured to be transmitted to the receivers.

(Conventional example 1)

In order to overcome the above stated problem, a cryptocommunication system is proposed using the NTRU cryptosystem described in the following. This 5 cryptocommunication system consists of an encrypting apparatus and a decrypting apparatus. The encrypting apparatus and the decrypting apparatus are connected to each other through a communication channel.

The encrypting apparatus generates n random numbers  $r_1$ , 10  $r_2, \dots, r_n$ , and encrypts plaintext m using an encryption key  $K_p$  stored in advance and the mentioned random numbers as parameters, in order to obtain n pieces of ciphertext  $c_1, c_2, \dots, c_n$ .

$$c_1 = E(m, K_p, r_1)$$

$$c_2 = E(m, K_p, r_2)$$

...

$$c_n = E(m, K_p, r_n)$$

Here, the equation  $C = E(M, K, R)$  shows that the ciphertext C is generated by encrypting the plaintext M using the encryption 20 key K and using the random number R as parameters.

Next, the encrypting apparatus transmits, to the decrypting apparatus, the generated ciphertext  $c_1, c_2, \dots, c_n$  through the communication channel.

The decrypting apparatus receives, through the 25 communication channel, n pieces of ciphertext  $c_1, c_2, \dots,$

$C_n$ , and decrypts the received ciphertext  $c_1, c_2, \dots, C_n$  using the decryption key  $K_s$  stored in advance, in order to obtain decrypted text  $m'_1, m'_2, \dots, m'_n$ .

$$m'_1 = D(c_1, K_s)$$

5       $m'_2 = D(c_2, K_s)$

...

$$m'_n = D(c_n, K_s)$$

Next, the decrypting apparatus considers that a decryption error has occurred if a single component in the decrypted text  
10       $m'_1, m'_2, \dots, m'_n$  is different.

This cryptocommunication system is inefficient in that it increases communications, even if it is capable of detecting the occurrence of decryption errors. In addition, there is a possibility of degrading the security for this  
15      cryptocommunication system, in which different random numbers are used as parameters for transmitting a plurality of pieces of ciphertext based on the same plaintext.

This is due to the possibility that, from  $n$  equations;

$$c_1 = E(m, K_p, r_1)$$

20       $c_2 = E(m, K_p, r_2)$

...

$$c_n = E(m, K_p, r_n),$$

the information on the plaintext  $m$  or on the random numbers  $r[1], r[2], \dots, r[n]$  are likely to be revealed to third parties.

25      The encryption attack using this disadvantage inherent in the

NTRU system is called "multiple transmission attack."

Specifically, it is known that the security is endangered when the decryption error detection is performed in the NTRU cryptosystem which is one of the detection error vulnerable 5 cryptosystems. Please refer, for a detailed description about the multiple transmission attack, to Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem," Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998.

10 As described in the above, the decryption error detection, performed in the NTRU cryptosystem, has a problem of increasing communications and lowering the security level.

(Conventional example 2)

15 A Japanese Laid-Open Publication No. 2000-216773 discloses the following technology for the purpose of providing a method and an apparatus for judging the correctness of the encrypted information in which receivers of the encrypted information can judge whether the decrypted information is 20 correct or not.

In this technology, a sender calculates a first hash value of plaintext using a predetermined hash value generation algorithm, and sends the first hash value with ciphertext resulting from encrypting the plaintext using an encryption 25 algorithm. A receiver, then, receives the ciphertext with the

first hash value, generates decrypted text by decrypting the ciphertext, calculates a second hash value of the decrypted text using the same hash value generation algorithm as is used for calculating the first hash value, compares the first hash 5 value and the second hash value, and judges that the decrypted text is correct only when the first and the second hash values match.

However, even when the above mentioned conventional technologies are used, it is difficult to completely avoid third 10 parties' attacks. A more secured cryptocommunication system is desired accordingly.

#### SUMMARY OF THE INVENTION

The object of the present invention, in order to solve 15 the above problem, is to provide a cryptocommunication system, a transmission apparatus, a reception apparatus, a method of cryptocommunication, program for a cryptocommunication, and a recording medium on which the program is recorded, that are more secure.

20 The object of the present invention is achieved by a cryptocommunication system including a transmission apparatus and a reception apparatus, the transmission apparatus encrypting plaintext to generate ciphertext, performing a one-way operation on the plaintext to generate 25 a first value, and transmitting the ciphertext and the first

value to the reception apparatus, the reception apparatus receiving the ciphertext and the first value, decrypting the ciphertext to generate decrypted text, performing the one-way operation on the decrypted text to generate a second value,  
5 and judging that the decrypted text matches the plaintext when the second value and the first value match, the transmission apparatus including: a first generating unit for generating first additional information; a first operation unit for performing an invertible operation on the plaintext  
10 and the first additional information to generate connected information; an encrypting unit for encrypting the connected information according to an encryption algorithm to generate the ciphertext; and a transmitting unit for transmitting the ciphertext, the reception apparatus comprising: a receiving unit for receiving the ciphertext; a second generating unit for generating second additional information which is identical to the first additional information; a decrypting unit for decrypting the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm  
15 so as to generate decrypted connected information; and a second operation unit for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.  
20

25 According to the structure, the transmission apparatus

enables to generate connected information by performing an invertible operation on the plaintext and on the first additional information, to generate encrypted connected information by encrypting the connected information, and to transmit the  
5 encrypted connected information. The reception apparatus enables to receive the connected information, to generate decrypted connected information by decrypting the received encrypted connected information, and to generate decrypted text by performing an inverse operation of the invertible operation  
10 on the decrypted connected information and on the second additional information. This realizes a more secured cryptocommunication system than the conventional ones.

Here, in the cryptocommunication system, the second generating unit synchronizes with the first generation unit so as to generate the second additional information which is identical to the first additional information.  
15

According to this structure, the second generating unit synchronizes with the first generating unit in order to generate second additional information which is identical to the first  
20 additional information, thereby enabling to obtain decrypted connected information which has the same content as the connected information.

Here, in the cryptocommunication system, the first generating unit generates a random number, and sets the generated  
25 random number as the first additional information.

According to this structure, the first generating unit can generate first additional information using a random number, thereby generating different additional information for each communication. This makes it difficult to infer first additional  
5 information from encrypted connected information.

Here, in the cryptocommunication system, the invertible operation unit bit-connects the plaintext with the first additional information so as to generate the connected information, and the second operation unit deletes the second  
10 additional information from the decrypted connected information to generate the decrypted text.

According to this structure, the invertible operation unit can generate connected information by bit-connecting the plaintext with the first additional information, and the inverse invertible operation unit can generate decrypted text by deleting the second additional information from the decrypted connected information. Therefore correct decrypted text is assured to be obtained from the decrypted connected information.  
15

## 20 BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings that illustrate a specific embodiment of the invention. In  
25 the drawings:

Fig. 1 is a block diagram showing a structure of a cryptocommunication system 1;

Fig. 2 is a block diagram showing a structure of an encrypting unit 105;

5 Fig. 3 is a block diagram showing a structure of a decrypting unit 202;

Fig. 4 is a flow chart showing an action performed by a transmission apparatus 10, the continuation thereof is shown in Fig. 5;

10 Fig. 5 is a flow chart showing an action performed by a transmission apparatus 10, which is a continuation from Fig. 4;

Fig. 6 is a flow chart showing an action performed by a reception apparatus 20;

15 Fig. 7 is an example of the conversion table used in the calculation method 6;

Fig. 8 is a block diagram showing a structure of a cryptocommunication system 1b which is a first modification example of the cryptocommunication system 1;

20 Fig. 9 is a flow chart showing an action performed by the cryptocommunication system 1b;

Fig. 10 is a block diagram showing a structure of a cryptocommunication system 1c which is a second modification example of the cryptocommunication system 1;

25 Fig. 11 is a flow chart showing an action performed by

the cryptocommunication system 1c;

Fig. 12 is a block diagram showing a structure of a cryptocommunication system 1d which is a third modification example of the cryptocommunication system 1;

5 Fig. 13 is a flow chart showing an action performed by the cryptocommunication system 1d; and

Fig. 14 is a table showing possible combinations between the modifications.

10 DESCRIPTION OF THE PREFERRED EMBODIMENTS

1. cryptocommunication system 1

The following is a description on a cryptocommunication system 1 which is one embodiment pertaining to the present invention.

15 1.1 the structure of the cryptocommunication system 1

A cryptocommunication system 1 is a system in which decryption error detection is enabled for the decryption error vulnerable cryptocommunication systems. As Fig. 1 shows, the 20 cryptocommunication system 1 consists of a transmission apparatus 10 and a reception apparatus 20, both of which are connected to each other through an internet 30.

The cryptocommunication system 1 uses the NTRU cyrptosystem which is one of the decryption error vulnerable 25 cryptosystems. Please refer to Jeffrey Hoffstein, Jill Pipher,

and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem," Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998 for detailed description about a method of generating NTRU ciphertext, and a method of generating 5 an encryption key and a decryption key for the NTRU cryptosystem.

The transmission apparatus 10 generates ciphertext by applying, to the plaintext stored in advance, the encryption algorithm according to the NTRU cryptosystem, and transmits the generated ciphertext to the reception apparatus 20. The 10 reception apparatus 20, in turn, receives the ciphertext, and generates decrypted text by applying, to the received ciphertext, the decryption algorithm according to the NTRU cryptosystem.

### 1.2 The structure of the transmission apparatus 10

The transmission apparatus 10 consists of a plaintext storage 101, an additional information generation unit 102, an information adding unit 103, a one-way operation unit 104, an encrypting unit 105, and a transmitting unit 106. The transmission apparatus 10 is concretely a computer system 15 composed of a microprocessor, ROM, RAM, a hard disk unit, a display unit, a key board, a mouse, a communication unit, and the like. The RAM or the hard disk unit stores computer program. The transmission apparatus 10 realizes its function by making 20 the microprocessor to work according to the computer program.

#### 25 (1) The plaintext storage 101

The plaintext storage 101 stores plaintext m in advance.

The plaintext m is composed of information with a fixed length.

(2) The additional information generation unit 102

The additional information generation unit 102 generates

5 additional information Ra which is a random number with a predetermined bit length of rLen, and outputs the generated additional information Ra to the information adding unit 103.

(3) The information adding unit 103

The information adding unit 103 reads out the plaintext

10 m from the plaintext storage 101, and receives the additional information Ra from the additional information generation unit 102.

Next, the information adding unit 103 connects the read plaintext m with the received additional information Ra by a bit-connecting method, so as to obtain resulting connected information F (m, Ra)=m||Ra.

Here, the operator "||" signifies a bit-connecting. The bit-connecting represents a single value which is a result from uniting two values, each represented as a bit row. In an example assuming that m=10, rLen=5, and Ra=7, the bit row representation for the plaintext m is "1010", and the bit row representation for the additional information Ra with a length of rLen is "00111". Thus, the result from the bit-connecting is "101000111" which means 327 in decimal notation.

25 Next, the information adding unit 103 outputs the

generated connected information  $F(m, Ra)$  to the encrypting unit 105.

(4) The one-way operation unit 104

The one-way operation unit 104 stores a hash function 5  $h$  which is a one-way operation.

Here, one-way operation is a function which is designed to calculate a value from an inputted value, but difficult to calculate the originally inputted value from the value. Further, an assumption is made about the hash function  $h$  used here that 10 it is assured to be difficult enough to obtain a value for the plaintext  $m$  using the value  $h(m)$ , and it is collide-free. For the details of the one-way operation, the hash function, the security of the hash function, and the collision-free characteristic of the hash function, refer to Tatsuaki Okamoto, 15 Hirosi Yamamoto, "Gendai Ango" (Modern cryptography), Series/Mathematics in Information Science, Sangyo-Tosho, 1997, pp.56, and pp.189-195.

The one-way operation unit 104 reads out the plaintext  $m$  from the plaintext storage 101, calculates a value  $h(m)$  from 20 the read plaintext  $m$  using the hash function  $h$ , and outputs the calculated value  $h(m)$  to the transmitting unit 106.

(5) The encrypting unit 105

The encrypting unit 105 consists of a random number generation unit 1051, an encryption key storage 1052, and an 25 encryption function unit 1053.

(the encryption key storage unit 1052)

The encryption key storage unit 1052 stores an encryption key  $K_p$  in advance.

(the random number generation unit 1051)

5 The random number generation unit 1051 generates a random number  $r$ , using a `rand()` which is a library function for the C language for example, and outputs the generated random number  $r$  to the encryption function unit 1053.

(the encryption function unit 1053)

10 The encryption function unit 1053 includes an encryption algorithm dedicated to the NTRU encryption cryptosystem in advance.

The encryption function unit 1053 receives a connected information  $F(m, Ra)$  from the information adding unit 103, 15 receives a random number  $r$  from the random number generation unit 1051, and reads out an encryption key  $K_p$  from the encryption key storage 1052.

Next, the encryption function unit 1053, using the random number  $r$  and the read encryption key  $K_p$ , encrypts the received 20 connected information  $F(m, Ra)$  according to the encryption algorithm, so as to generate encrypted connected information  $E(F(m, Ra), K_p, r)$ , and outputs the generated encrypted connected information  $E(F(m, Ra), K_p, r)$  to the transmitting unit 106.

#### (6) The transmitting unit 106

25 The transmitting unit 106 receives the encrypted connected

information E ( $F(m, Ra)$ ,  $K_p$ ,  $r$ ) and the value  $h(m)$ , and transmits these, through the internet 30, to the reception apparatus 20.

1.3 The structure of the reception apparatus 20

The reception apparatus 20 consists of a receiving unit 201, a decrypting unit 202, an information removing unit 203, a one-way operation unit 204, a comparison unit 205, a decrypted text storage 206, and a comparison result storage 207. The reception apparatus 20 is specifically the same computer system as the transmission apparatus 10.

10 (1) The receiving unit 201

The receiving unit 201 receives, from the transmission apparatus 10, the encrypted connected information E ( $F(m, Ra)$ ,  $K_p$ ,  $r$ ) and a value  $h(m)$  through the internet 30, and outputs the received encrypted connected information E to the decrypting unit 202, and outputs the received value  $h(m)$  to the comparison unit 205.

(2) The decrypting unit 202

The decrypting unit 202 consists of a decryption key storage 2021 and a decryption function unit 2022.

20 (The decryption key storage 2021)

The decryption key storage unit 2021 stores a decryption key  $K_s$  in advance.

(The decryption function unit 2022)

The decryption function unit 2022 stores a decryption algorithm which is an inversed form of the encryption algorithm

which is included in the encryption function unit 1053.

The decryption function unit 2210 receives the encrypted connected information  $E(F(m, Ra), Kp, r)$  from the receiving unit 201, and reads out the decryption key  $Ks$  from the decryption key storage 2021.

Next, the decryption function unit 2210, using the read decryption key  $Ks$ , decrypts the received encrypted connected information  $E(F(m, Ra), Kp, r)$  according to the decryption algorithm, so as to generate a decrypted connected information  $D(E(F(m, Ra), Kp, r), Ks)$ , and outputs the decrypted connected information to the information removing unit 2250.

### (3) The information removing unit 203

The information removing unit 203 stores a bit length  $rLen$  in advance.

The information removing unit 203 receives the decrypted connected information  $D(E(F(m, Ra), Kp, r), Ks)$  from the decrypting unit 202, and removes the additional information  $Ra$  from the decrypted connected information, by removing a bit row of the  $rLen$  bit length from the end of the received decrypted connected information  $D(E(F(m, Ra), Kp, r), Ks)$ , generates decrypted text from the remaining information after the additional information  $Ra$  is removed from the decrypted connected information, and outputs the generated decrypted text  $m'$  to the one-way operation unit 204. The information removing unit 203 also writes the generated decrypted text  $m'$  on the

decrypted text storage 206.

(4) The one-way operation unit 204

The one-way operation unit 204 stores, in advance, the same hash function  $h$  which is included in the one-way operation unit 104.

The one-way operation unit receives the decrypted text  $m'$  from the information removing unit 203, hashes the received decrypted text  $m'$  according to the hash function  $h$  to generate a functional value  $h(m')$  and outputs the value  $h(m')$  to the comparison unit 205.

(5) The comparison unit 205

The comparison unit 205 receives the value  $h(m)$  from the receiving unit 201, and the value  $h(m')$  from the one-way operation unit 204.

Next, the comparison unit 205 compares the value  $h(m)$  with the value  $h(m')$ , judges whether the two values match, and generates the comparison result  $j$  which shows whether matching or non-matching. Specifically, The comparison unit 205, when they match, generates a comparison result which shows  $j=1$ , and when they do not match, generates a comparison result which shows  $j=0$ , and write the generated comparison result  $j$  on the comparison result storage 207.

(6) The decrypted text storage 206

The decrypted text storage 206 has an area for storing decrypted text.

(7) The comparison result storage 207

The comparison result storage 207 has an area for storing a comparison result  $j$ .

1.4 The action of the transmission apparatus 10

5 The following is a description of the action that the transmission apparatus 10 performs, with reference to the follow charts shown in Fig. 4 and Fig. 5.

The additional information generation unit 102 generates additional information  $R_a$ , and outputs the generated additional 10 information  $R_a$  to the information adding unit 103 (Step S101).

Next, the information adding unit 103 reads out the plaintext  $m$  from the plaintext storage 101 (step S102), receives the additional information  $R_a$  from the additional information generation unit 102 (step S103), generates connected 15 information  $F(m, R_a)$  by uniting the plaintext  $m$  with the additional information  $R_a$ , and outputs the generated connected information  $F(m, R_a)$  to the encrypting unit 105 (step S104).

Next, the encrypting unit 105 receives the connected information  $F(m, R_a)$ , generates encrypted connected information 20  $E(F(m, R_a), K_p, r)$  by applying the encrypting algorithm  $E$  to the received connected information  $F(m, R_a)$  (step S105), and outputs the generated encrypted connected information  $E(F(m, R_a), K_p, r)$  to the transmitting unit 106 (step S106).

Next, the one-way operation unit 104 reads out the 25 plaintext  $m$  from the plaintext storage 101 (step S107) calculates

a value  $h(m)$  from the plaintext  $m$  using the hash function  $h$  (step S108), and outputs the calculated value  $h(m)$  to the transmitting unit 106 (step S109).

The transmitting unit 106 receives the encrypted connected information  $E(F(m, Ra), Kp, r)$  and the value  $h(m)$ , and transmits, through the internet 30, the received encrypted connected information and the value to the reception apparatus (step S110).

#### 1.5 The action that the reception apparatus 20 performs

The following is a description of the action that the reception apparatus 20 performs, with reference to the flow chart shown in Fig. 6.

The receiving unit 201, from the transmission apparatus 10, receives encrypted connected information  $E(F(m, Ra), Kp, r)$  and a value  $h(m)$  through the internet 30 (step S151), outputs the received encrypted connected information to the decrypting unit 202, and the received value to the comparison unit 205 (step S152).

The decrypting unit 202 receives the encrypted connected information  $E(F(m, Ra), Kp, r)$ , and generates decrypted connected information  $D(E(F(m, Ra), Kp, r))$  by applying the decryption algorithm  $D$  to the received encrypted connected information  $E(F(m, Ra), Kp, r)$  (step S153), and outputs the decrypted connected information to the information removing unit 203 (step S154).

The information removing unit 203 receives the decrypted

connected information  $D(E(F(m, Ra), K_p, r))$ , and removes the additional information  $Ra$  from the received decrypted connected information so as to generate decrypted text  $m'$  (step S155), outputs the generated decrypted text  $m'$  to the one-way operation unit 204, and writes the generated decrypted text  $m'$  on the decrypted text storage 206 (step S156).

The one-way operation unit 204 receives the decrypted text  $m'$ , hashes the received decrypted text  $m'$  according to the hash function  $h$  to calculate a value  $h(m')$ , and outputs the calculated value  $h(m')$  to the comparing unit 205 (step S157).

The comparing unit 205 receives the value  $h(m)$  and the value  $h(m')$ , compares the two values to judge whether the two match, generates a comparison result  $j$  either showing matching or non-matching, and writes the generated comparison result  $j$  on the comparison result storage 207 (step S158).

#### 1.6 The comparison of action between the embodiment and the conventional examples

The following is a description of decryption error detection according to the embodiment of the present invention.

20 The decryption error detection is then compared with those used in the conventional technologies.

When there is not decryption error, the comparison result  $j$  which is to be outputted from the comparison unit 205 of the reception apparatus 20 is always 1.

25 The possibility that the comparison result  $j$  is 1, that

is, the possibility that  $h(m')$  generated from the one-way operation unit 204 of the reception apparatus 20 happens to be equal to  $h(m)$  generated from the one-way operation unit 104 of the transmission apparatus 10 is as follows:

5 For the one-way operation unit 104 and the one-way operation unit 204 using the hash function outputting a hash value of the length of  $k$  bits, there are  $2^k$  ways of hash value with  $k$  bits. Therefore the possibility thereof is  $2^{-k}$ .

Therefore, if there is actually a decryption error, the 10 possibility that the decryption error is detected by examining the comparison result  $j$  generated by the reception apparatus 20 is  $1-2^{-k}$ .

For example, when assumption is made that a hash function is SHA-1, the SHA-1 has at least 160 bits of output. Therefore, 15 the possibility will be  $1-2^{-160}$ , which means that almost all the detection errors can be detected.

Moreover, the communications through the internet 30 is a sum of the bit length of the ciphertext outputted from the encrypting unit 105 and the bit length of the hash value outputted 20 from the one-way operation unit 104. Generally speaking, the output bit length for a hash function is smaller than that for inputted data. Therefore, it is unlikely that the communications in this example is more than twice as many as the output bit length for the ciphertext.

25 For example, when the hash function to be used is SHA-1

this holds true since most cryptosystems including the NTRU cryptosystem use ciphertext length of 160 bits or more.

The communications in the data cryptosystem according to the conventional example 1 has several times as many as the 5 output bits length of the ciphertext. It can be concluded, therefore, that the communications is reduced for the present embodiment, therefore enhancing the communication efficiency.

Further, as for the security consideration, the present embodiment makes it difficult to infer the inputted value from 10 the outputted value. Moreover, the present embodiment is not designed, unlike the conventional example 1, to transmit the same plaintext more than one time. Therefore, an adequate security level is insured in the present embodiment. In addition, in a case in which the protocol is adopted for re-transmitting the same data again by re-transmission request, after the decryption error detection is performed, the present embodiment 15 is more resistant to the multiple transmission attack than the data cryptosystem described in the conventional example 1, since the present embodiment adds a random number to plaintext before 20 encrypting.

Moreover, the conventional technology encrypts plaintext from its intact condition. This increases the possibility of being decrypted by a third party who intercepts the communication channel, when the sender resends, upon request from the receiver, 25 ciphertext generated from the same plaintext. That is, there

is a possibility that a third party can intercept and decrypt the several pieces of ciphertext into the plaintext. (This phenomenon is called multiple transmission attack as is mentioned in the conventional example 1.)

5 On the contrary, the present embodiment is able to set different additional information Ra for each communication. This enables to create a different m||Ra value for same plaintext every time the sender has to resend ciphertext. This reduces the possibility of being illegally decrypted by a third party  
10 attempting to perform a multiple transmission attack.

Moreover, the low transmission quality of the transmission channel enables to detect a difference between the original plaintext and the decrypted text, when the bit is lost or garbled, just as mentioned in the above.

15  
2. Modifications of the cryptocommunication system 1  
The following is a description of modifications for the cryptocommunication system 1.

20 2.1 modifications on the additional information  
In the cryptocommunication system 1, the additional information generation unit 102 is to generate additional information Ra which is a random number. However, it is also possible to be replaced by time stamp information or counter  
25 information. To summarize, the additional information that is

generated by the additional information generation unit 102 can be any type of information if only it yields a different value every time it is used.

The time stamp information represents current time when  
5 the additional information generation unit 102 generates a piece of additional information, and is specifically composed of information showing year, month, day, hour, minute, second, and millisecond, in a fixed length.

The counter information is numerical information in  
10 fixed digits, and is designed to add 1 every time it is used.

## 2.2 modifications for calculating the connected information $F(m, Ra)$

In the cryptocommunication system 1, the information adding unit 103 calculates connected information  $F(m, Ra) = m || Ra$ ,  
15 by uniting plaintext  $m$  with additional information  $Ra$ . However, the calculation method can be other than this method if it is invertible in such a way that  $m$  can be converted in the reverse direction based on the additional information.

20 Examples of the other calculation methods are listed in the following including the calculation method of the embodiment.

In order to extract only the plaintext by removing the additional information from the connected information, an  
25 inverse operation is performed.

(1) calculation method 1

The calculation method 1 is expressed as connected information  $F(m, Ra) = m \parallel Ra$ , where " $\parallel$ " signifies a bit-connecting. This is a calculation for obtaining plaintext 5 for the embodiment.

Note that an expression "connected information  $F(m, Ra)=Ra \parallel m$ " can be alternatively used for the expression described above.

Further, the plaintext  $m$  is divided into several pieces 10 of partial plaintext information, each having length of 4 bits. In the same way, the additional information, too, is divided into several pieces of partial additional information, each having length of 4 bits. Then, connected information may be obtained by uniting the pieces of partial plaintext information 15 and the pieces of partial additional information alternately. Generally speaking, a length of plaintext  $m$  is greater than a length of additional information. Therefore, the connected information usually ends with partial plaintext information.

(2) calculation method 2

20 The calculation method 2 is expressed as "connected information  $F(m, Ra)=m (+) Ra$ ," where "(+)" signifies an exclusive OR, with its inverse operation being expressed as "decrypted text  $m' =$  connected information  $F(+) Ra$ ."

(3) Calculation method 3

25 The calculation method 3 is expressed as "connected

information  $F(m, Ra) = m + Ra$ , " with its inverse operation being expressed as "decrypted text  $m' = \text{connected information } F - Ra$ ."

(4) calculation method 4

The calculation method 4 is expressed as "connected

5 information  $F(m, Ra) = m \times Ra \bmod p$ " where  $p$  is a prime number greater than  $m$ .

The inverse operation is performed as follows:

Decrypted text  $m' = \text{connected information } F / Ra \bmod p$

(5) Calculation method 5

10 The calculation method 5 is expressed as "connected information  $F(m, Ra) = \text{BitPerm} [Ra] (m)$ , " where  $\text{BitPerm} [Ra] (m)$  is an operation for replacing the bit expression  $m$  based on  $Ra$ .

The specific operation methods are shown in the following:

15 (5-1) calculation method 5-1

This expression is to bit-rotate  $m$  by  $Ra$  bits.

For example, if  $m$  is assumed to be "1111000011110000", and  $Ra$  is assumed to be  $Ra = 3$  (in decimal notation), then the  $m$  after replacement can be expressed as  $m = 1000011110000111$ .

20 Here, the reverse bit rotation is also possible.

The inverse operation is performed by rotating the connected information  $F$  in a reverse direction by  $Ra$  bits.

(5-2) calculation method 5-2

In this method,  $m$  is replaced according to the calculation

25 algorithm. In other words, an operation is performed first by

making Ra an inputted value, and then m is replaced based on the calculation result.

The above-described two calculation method is described in the following using examples.

5 (example)

Ra is assumed to be 128-bit-length. The hash value of 16-bit-length is calculated from Ra using a hash function. Next, m is bit-rotated by the obtained hash value as shown in the calculation method 5-1.

10 The inverse operation is performed as follows:

The connected information F is replaced according to the calculation algorithm. In other words, the operation is performed making the Ra an inputted value. Then the connected information F is replaced based on the operation result, in order to obtain decrypted text m'.

15 (example)

Ra is assumed to be 128-bit-length. a 16-bit-length hash value is calculated from Ra using a hash function. Next, as the calculation method 5-1, the connected information F is bit-rotated in a reverse direction by the obtained hash value.

20 (5-3) calculation method 5-3

In the calculation method 5-3, several pieces of partial information is generated by dividing m into 4 bit length. Next, each piece of partial information is replaced using the replacement table for 4 input-output bit length corresponding

to Ra.

Here, the replacement table includes 16 sets before-conversion bit row with 4 bit length, and the corresponding after-conversion bit row with 4 bit length.

5 In the replacement table for Ra of a certain value (e.g. "1"), 16 before-conversion bit rows are expressed as 0000, 0001, 0010, ..., 1110, and 1111. The corresponding 16 after-conversion bit rows are 1111, 1110, 1101, ..., 0001 and 0000.

10 For a different value of Ra (e.g. 2), the corresponding replacement table thereto has 16 after-conversion bit rows: 1111, 1110, 1101, ..., 0000, and 0001.

In the above fashion, more than one type of replacement table is made possible for each value of Ra.

The inverse operation is performed as follows.

15 Connected information F is divided into 4 bits, in order to generate several pieces of partial connected information. Next, the replacement in a reverse direction is performed for each piece of partial connected information, using the replacement table for 4 input-output bit length corresponding  
20 to a Ra.

#### (6) calculation method 6

The calculation method 6 is expressed as "connected information  $F(m, Ra) = Tab[Ra](m)$ ," where  $Tab[Ra](m)$  means to convert m according to the conversion table Tab.

25 For example, when m is assumed to have 8-bit-length, each

m is converted according to the table Tab as shown in Fig. 7 which is stored for each Ra. The conversion table Tab includes 256 sets of 8-bit value and 8-bit value.

For an example in which m=1, plaintext m is converted  
5 into 39 according to the conversion table Tab shown in Fig.  
7.

The inverse operation is performed as follows:

Connected information F is converted in the reverse direction to the above, according to the conversion table Tab.

10

2.3 Modification examples of the cryptocommunication system in which additional information is shared

The following is a description on modification examples for the cyrptocommunication system in which additional  
15 information is shared.

(1) a first modification example

As a first modification example, a cryptocommunication system 1b is described which is a modified form of the cryptocommunication system 1.

20 (a structure of the cryptocommunication system 1b)

The cryptocommunication system 1b consists of a transmission apparatus 10b and a reception apparatus 20b, as shown in Fig.  
8.

25 The transmission apparatus 10b and the reception apparatus 20b each have the same structure as the transmission apparatus

10 and the reception apparatus 20 respectively, that constitutes  
the cryptocommunication system 1. The following is a description  
of the transmission apparatus 10b and the reception apparatus  
20b, with an emphasis on the difference between the transmission  
5 apparatus 10 and the reception apparatus 20.

The transmission apparatus 10b is further equipped with  
a synchronizing unit 107. In addition, the transmission  
apparatus 10b is equipped with an additional information  
generation unit 102b instead of the additional information  
10 generation unit 102 which the cryptocommunication system 1 has.  
In addition, the reception apparatus 20b is further equipped  
with a synchronizing unit 208 and an additional information  
generation unit 209. The synchronizing unit 107 and the  
synchronizing unit 208 are connected to each other through the  
15 dedicated line 40b.

The synchronizing unit 107 generates a random number XR,  
and outputs the generated random number XR through the dedicated  
line 40b to the synchronizing unit 208. The synchronizing unit  
107 further outputs the generated random number XR to the  
20 additional information generation unit 102.

The additional information generation unit 102, upon  
receiving the random number XR from the synchronizing unit 107,  
generates additional information Ra using the received random  
number XR, and outputs the generated additional information  
25 Ra to the information adding unit 103. Here, an assumption is

made that the random number XR is used as the additional information Ra without being processed, which is one example of generating additional information Ra from the random number XR.

5       The synchronizing unit 208 receives the additional information XR through the dedicated line 40b, and outputs the received additional information XR to the additional information generation unit 109.

The additional information generation unit 209, upon  
10 receiving the random number XR from the synchronizing unit 208,  
generates additional information Ra using the received random  
number XR, and outputs the generated additional information  
Ra to the information removing unit 203. Here, an assumption  
is made that the random number XR is used as the additional  
15 information Ra without being processed, which is one example  
of generating additional information Ra from the random number  
XR.

(action of the cryptocommunication system 1b)

The action that the cryptocommunication system 1b performs  
20 is described in the following with reference to the flow chart  
shown in Fig. 9.

Note that the focus here is on the differences between  
the cryptocommunication systems 1b and 1, since the most of  
the action are the same between the two systems.

25       The synchronizing unit 107 generates a random number XR

(Step S201), and outputs the generated random number XR through the dedicated line 40b to the synchronizing unit 208 (Step S202). The synchronizing unit 107 further outputs the generated random number XR to the additional information generation unit 102  
5 (step S203).

The additional information generation unit 102, upon receiving the random number XR from the synchronizing unit 107, generates additional information Ra using the received random number XR, and outputs the generated additional information  
10 Ra to the information adding unit 103 (step S203).

The synchronizing unit 208 receives the random number through the dedicated line 40b, and outputs the received random number XR to the additional information generation unit 209  
15 (step S202).

The additional information generation unit 209, upon receiving the random number XR, generates additional information Ra using the received random number XR (step S204), and outputs the generated additional information Ra to the information removing unit 203 (step S205). The information  
20 removing unit 203 receives the additional information Ra (step S205), and generates decrypted text  $m'$  from decrypted connected information using the received additional information Ra (step S206).

(2) a second modification example

25 A cryptocommunication system 1c is described which is

a second modification example of the cryptocommunication system

1.

(a structure of the cryptocommunication system 1c)

The cryptocommunication system 1c consists of a  
5 transmission apparatus 10c and a reception apparatus 20c, as  
shown in Fig. 10.

The transmission apparatus 10c and the reception apparatus  
20c each have the same structure as the transmission apparatus  
10 and the reception apparatus 20 for the cryptocommunication  
10 system 1.

The transmission apparatus 10c, instead of the additional  
information generation unit 102 and the transmitting unit 106,  
is equipped with an additional information generation unit 102c  
and a transmitting unit 106c. The reception apparatus 20c,  
15 instead of the information removing unit 203 and the receiving  
unit 201, is equipped with an information removing unit 203c  
and a receiving unit 201c.

The additional information generation unit 102c, the  
transmitting unit 106c, the information removing unit 203c,  
20 and the receiving unit 201c each have the same structure as  
the additional information generation unit 102, the  
transmitting unit 106, the information removing unit 203, and  
the receiving unit 201 respectively. Therefore, the focus will  
be on the differences in the following description.

25 The additional information generation unit 102c outputs

the generated additional information Ra to the transmitting unit 106c.

The transmitting unit 106c receives additional information Ra from the additional information generation unit 102c, and transmits the received additional information Ra to the reception apparatus 20c through the internet 30.

The receiving unit 201c receives the additional information Ra through the internet 30 from the transmission apparatus 10c, and outputs the received additional information 10 Ra to the information removing unit 203c.

The information removing unit 203c receives the additional information Ra from the receiving unit 201, and generates decrypted text m' from decrypted connected information using the received additional information Ra.

15 (action of the cryptocommunication system 1c)

The action that the cryptocommunication system 1c performs is described in the following with reference to the flow chart shown in Fig. 11.

Note that the focus will be on the differences between 20 the two systems, since the most of the action of the cryptocommunication system 1c is the same as the cryptocommunication system 1.

The additional information generation unit 102c generates additional information Ra, and outputs the generated additional 25 information Ra to the transmitting unit 106c (step S221).

The transmitting unit 106c receives the additional information Ra from the additional information generation unit 102c, and transmits the received additional information Ra through the internet 30 to the reception apparatus 20c (step 5 S222).

The receiving unit 201c receives the additional information Ra through the internet 30 from the transmission apparatus 10c, and outputs the received additional information Ra to the information removing unit 203c (step S222).

10 The information removing unit 203c receives the additional information Ra from the receiving unit 201 (step S223), and generates decrypted text  $m'$  from the decryption connected information using the received additional information Ra (step S224).

15 (3) a third modification example

The following is a description on a cryptocommunication system 1d, which is a third modification example of the cryptocommunication system 1.

(a structure of the cryptocommunication system 1d)

20 The cryptocommunication system 1d consists of a transmission apparatus 10d and a reception apparatus 20d, as shown in Fig. 12.

The transmission apparatus 10d and the reception apparatus 20d each have the same structure as the transmission apparatus 25 10 and the reception apparatus 20 that compose the

cryptocommunication system 1.

The transmission apparatus 10d , instead of the additional information generation unit 102, the encrypting unit 105, and the transmitting unit 106, is equipped with an additional 5 information generation unit 102d, an encrypting unit 105d, and a transmitting unit 106d. The reception apparatus 20d, instead of the decrypting unit 202, the information removing unit 203, and the receiving unit 201, is equipped with a decrypting unit 202d, an information removing unit 203d, and a receiving unit 10 201d.

The additional information generation unit 102d, the encrypting unit 105d, the transmitting unit 106d, the decrypting unit 202d, the information removing unit 203d, and the receiving unit 201d, each have the same structure as the additional 15 information generation unit 102, the encrypting unit 105, the transmitting unit 106, the decrypting unit 202, the information removing unit 203, and the receiving unit 201 respectively. The following description focuses on the differences accordingly.

20 The additional information generation unit 102d generates additional information Ra, and outputs the generated additional information Ra to the encrypting unit 105d.

The encrypting unit 105d, upon receiving the additional information Ra from the additional information generation unit 25 102d, applies an encryption algorithm to the received additional

information Ra, so as to generate encrypted additional information E(Ra, Kp, r2). Here, r2 is a random number as r. Next, the encrypting unit 105d outputs the generated encrypted additional information E(Ra, Kp, r2) to the transmitting unit 5 106d.

The transmitting unit 106d receives the encrypted additional information E(Ra, Kp, r2) from the encrypting unit 105d, and transmits the received encrypted additional information E(Ra, Kp, r2) through the internet 30 to the reception 10 apparatus 20d.

The receiving unit 201d receives, through the internet 30, the encrypted additional information E(Ra, Kp, r2) from the reception apparatus 20d, and outputs the received encrypted additional information E(Ra, Kp, r2) to the decrypting unit 202d.

The decrypting unit 202d receives the encrypted additional information E(Ra, Kp, r2) from the receiving unit 201d, and generates decrypted additional information D(E(Ra, Kp, r2), Ks) by applying a decryption algorithm to the received encrypted additional information E(Ra, Kp, r2). Next, the decrypting unit 20 202d outputs the generated decrypted additional information D(E(Ra, Kp, r2), Ks) to the information removing unit 203d.

The information removing unit 203d receives decrypted additional information D(E(Ra, Kp, r2), Ks) from the decrypting unit 202d, and generates decrypted text m' from decrypted 25 connected information D(E(F(m, Ra), Kp, r), Ks), using the

received decrypted additional information  $D(E(Ra, Kp, r2), Ks)$ .

(action of the cryptocommunication system 1d)

The action that the cryptocommunication system 1d performs is described in the following with reference to the flow chart 5 shown in Fig. 13.

Since the action of the cryptocommunication system 1d is mostly the same as that of the cryptocommunication system 1, the focus in the following description is on their differences.

The additional information generation unit 102d generates 10 additional information Ra, and outputs the generated additional information Ra to the encrypting unit 105d (step S241).

The encrypting unit 105d receives additional information Ra from the additional information generation unit 102d, generates encrypted additional information  $E(Ra, Kp, r2)$  by 15 applying an encryption algorithm to the received additional information Ra, and outputs the generated encrypted additional information  $E(Ra, Kp, r2)$  to the transmitting unit 106d (step S242).

The transmitting unit 106d receives the encrypted 20 additional information  $E(Ra, Kp, r2)$  from the encrypting unit 105d, and transmits the received encrypted additional information  $E(Ra, Kp, r2)$  through the internet 30 to the reception apparatus 20d (step S243).

The receiving unit 201d receives, from the reception 25 apparatus 20d, the encrypted additional information  $E(Ra, Kp, r2)$

through the internet 30, and outputs the received encrypted additional information  $E(Ra, Kp, r2)$  to the decrypting unit 202d (step S243).

The decrypting unit 202d receives, encrypted additional information  $E(Ra, Kp, r2)$  from the receiving unit 201d, and generates decrypted additional information  $D(E(Ra, Kp, r2), Ks)$  by applying a decryption algorithm to the received encrypted additional information  $E(Ra, Kp, r2)$ . Then, the decrypting unit 202d outputs the generated decrypted additional information  $D(E(Ra, Kp, r2), Ks)$  to the information removing unit 203d (step S244).

The information removing unit 203d receives, from the decrypting unit 202d, the decrypted additional information  $D(E(Ra, Kp, r2), Ks)$  (step S245), and generates decrypted text  $m'$  from the decrypted connected information  $D(E(F(m, Ra), Kp, r), Ks)$  using the received encrypted additional information  $D(E(Ra, Kp, r2), Ks)$  (Step S246).

#### 2.4 Feasible combination between modifications

Feasible combinations between the modifications regarding the additional information, the modifications for the calculation of the connected information  $F(m, Ra)$ , and the modification examples of the cryptocommunication system in which the additional information is shared are described in the following with reference to the table shown in Fig. 14.

As the table in Fig. 14 shows, each modification for

additional information (i.e. a random number, a time stamp, and a counter) can be used with all the modifications for calculating connected information  $F(m, Ra)$ , or with the modification examples of the cryptocommunication system in 5 which the additional information is shared.

Further, the modification in which  $m||Ra$  is used for calculating the connected information is applicable to cryptocommunication systems 1, and 1b-1d, as Fig. 14 shows.

In addition, among the modifications for calculating 10 connected information  $F(m, Ra)$ ,  $m(+)\text{Ra}$ ,  $m\times\text{Ra}$ ,  $m \bmod p$ , BitPerm [Ra] (m), Tab[Ra] (m) methods, as Fig. 14 shows, are applicable to the cryptocommunication systems 1b-1d.

### 3. Other modification examples

So far, the present invention was described based on the 15 embodiment. The present invention is not limited to the described embodiment, and also includes other cases described in the following.

(1) The cryptocommunication system 1 may be structured in the following way. The one-way function unit 104 of the 20 transmission apparatus 10 receives connected information  $F(m, Ra)$  from the information adding unit 103, and hashes the received connected information  $F(m, Ra)$  according to the hash function  $h$  to generate a functional value  $h(F(m, Ra))$ , and transmits the functional value  $h(F(m, Ra))$  through the 25 transmitting unit 106, the internet 30, and the receiving unit

201, to the comparing unit 205.

The one-way function unit 204 of the reception apparatus 20 receives decrypted connected information  $D(E(F(m, Ra), Kp, r), Ks)$  from the decrypting unit 202, and hashes 5 the received  $D(E(F(m, Ra), Kp, r), Ks)$  according to the hash function  $h$ , so as to generate a functional value  $h(D(E(F(m, Ra), Kp, r), Ks))$ , and outputs the generated functional value  $h(D(E(F(m, Ra), Kp, r), Ks))$  to the comparing unit 205. The comparing unit 205 compares the functional value  $h(F(m, Ra))$  10 and the functional value  $h(D(E(F(m, Ra), Kp, r), Ks))$  and judges whether the two match.

In the above way, the judgement is performed as to whether the plaintext has been correctly decrypted or not.

(2) Moreover, the cryptocommunication system 1 may be 15 structured in the following way.

The information adding unit 103 of the transmission apparatus 10, using  $G$  which is a different invertible operation from  $F$ , generates connected information  $G(m, Ra)$ . Here, an example of  $G$  is  $G=Ra \mid | m$ . Next, the information adding unit 103 20 outputs the generated connected information  $G(m, Ra)$  to the one-way function unit 104. The one-way function unit 104 receives the connected information  $G(m, Ra)$  from the information adding unit 103, and hashes the received connected information  $G(m, Ra)$  according to the hash function  $h$ , so as to generate a functional 25 value  $h(G(m, Ra))$ , and transmits the generated functional value

$h(G(m, Ra))$  through the transmitting unit 106, the internet 30, and the receiving unit 201, to the comparing unit 205.

Further, the information removing unit 205 of the reception apparatus 20, using the decrypted text  $m'$ , a random number  $Ra$ , and the  $G$ , generates connected information  $G(m', Ra)$ , and transmits the generated  $G(m', Ra)$  to the one-way function unit 204. Here, the information removing unit 203 shares the same random number  $Ra$  with the transmission apparatus 10, as shown in the first modification example. The one-way function unit 204 receives the connected information  $G(m', Ra)$ , and hashes the received connected information  $G(m', Ra)$  according to the hash function  $h$ , so as to generate a functional value  $h(G(m', Ra))$ , and outputs the generated functional value  $h(G(m', Ra))$  to the comparing unit 205. The comparing unit 205 compares the functional value  $h(G(m, Ra))$  and the functional value  $h(G(m', Ra))$  to see whether the two match.

In the above way, the judgment is performed as to whether the plaintext has been decrypted correctly.

(3) The encryption algorithm and the decryption algorithm are not limited to those described in the embodiment, and other crypto-algorithms are also possible. For example, ordinary cryptosystems such as the DES cryptosystem, the RSA cryptosystem, and the ElGamal cryptosystem can also be used.

In addition, for the one-way operation unit 104, cryptosystem functions used for the ordinary cryptosystems can

be also used as well as the hash functions.

For a detailed description about the DES cryptosystem, the RSA cryptosystem, and the ElGamal cryptosystem, please refer to Tatsuaki Okamoto, Yamamoto Hirosi, "Gendai Ango" (Modern Cryptography), Series/Mathematics in Information Science, Sangyo Tosho, 1997.

Further, it can be also arranged so that each couple of transmitting users and receiving users can have a different one-way operation, instead of all the users in one system share one one-way operation.

(4) In the present embodiment, the transmission apparatus 10 and the reception apparatus 20 are connected to each other through the internet 30. However connecting means is not limited to the internet, and can also be a dedicated line, or by over-the-air.

(5) The present invention can be the method described above, or can be computer program enabling the method by a computer. Or the present invention can be digital signals comprised of the computer program.

Further, the present invention can be a recording medium which can be read from using a computer, such as a flexible disk, a hard disk, CD-ROM, MO, a DVD, DVD-ROM, DVD-RAM, or semiconductor memory, which stores the computer program or the digital signals. Or the present invention can also be the computer program or the digital signals recorded on these recording media.

Further, the present invention can transmit the computer program or the digital signals through a network represented by electric communication lines, over-the-air, cable transmission lines, or the internet, for example.

5        Further, the present invention can be a computer system equipped with a microprocessor and memory, in which the memory stores computer program, and the microprocessor can work according to the computer program.

In addition, another computer system which is independent  
10 from the computer system described can realize the tasks, by transmitting the computer program or the digital signals stored in the recording media, or by transmitting the computer program or the digital signals through the network and the like.

15      (6) The stated embodiment and the modifications can be combined to each other.

Although the present invention has been fully described by way of examples with reference to the accompanying drawings, it is to be noted that various changes and modifications will be apparent to those skilled in the art. Therefore, unless  
20 otherwise such changes and modifications depart from the scope of the present invention, they should be construed as being included therein.